Some New Challenges of Cybercrime and Reasons Why Regulations are Outdated

Anri Nishnianidze, PhD student
Grigol Robakidze University, Georgia

Doi: 10.19044/esipreprint.9.2022.p288

Approved: 18 September 2022
Posted: 20 September 2022

Cite As:
Nishnianidze A.(2022). *Some New Challenges of Cybercrime and Reasons Why Regulations are Outdated.* ESI Preprints. https://doi.org/10.19044/esipreprint.9.2022.p288

Abstract

Purpose – The purpose of the research is to show what cybercrime is and how the arsenal of cybercriminals has evolved and legal regulations that exist today no longer respond to the challenges that would make the battle against cybercrime effective. Design/methodology/approach – The author of the research searched for the latest legal and multidisciplinary literature on the issue of cybercrime. Using various scientific methods, the mentioned literature was analyzed and summarized to present the essence and problems of fighting against cybercrime. Findings – In the conditions of modern technological development, there are many benefits along with negative facts. Cyberspace is not a safe place for the majority of the population. During the search process, it appeared that, with the arrival of each new day, the arsenal of cybercriminals is getting richer, to which the law enforcement structures do not have an appropriate response. Consequently, the process of battling cybercrime becomes difficult due to outdated legal regulations. Research limitations/implications – The research examined the latest opinions that are being debated in international legal circles. The problems that are on the agenda and which are important to solve have appeared. Accordingly, the paper offers the latest ways to correct the current situation, make recommendations and solve existing problems. Originality/value – Cyberspace is the most important space for many people, also for private and

public structures. Solving the current issues on the agenda is important to make working in cyberspace safe for each person and organization.

Keywords: Cybercrime, Computer Crimes, Virtual Criminology, Cyberspace, Cyber Security

Introduction

In modern times, cybercrime is rightly considered as one of the newest and most important challenges due to its complexity and ability to evolve (Choi et al., 2020). In a short period, cybercriminals are armed with new tools, the battle against which is a special difficulty for the law enforcement structures, because the mentioned crime is a type of crime that needs special knowledge to battle against it: computer data processing, knowledge of programming languages, etc. Because, the aforementioned is the core of the arsenal of cybercriminals (Hutchings et al., 2019). Cybercriminals can cause harm both to a specific person personally, also to private organizations or state structures. In this process, they use several weapons that technological progress has given to them, and the battle against them is not effective in many cases, because the response to the crime is not immediate (Ec-Council, 2016).

To create an idea about cybercrime for a researcher who does not have sufficient technical education, it is enough to familiarize himself with the encyclopedia of cybercrime, as a result of which the researcher will see how rich the arsenal of the cybercriminal is (Marion & Twede, 2020). The motivations of cybercriminals are different in every case, in some cases, they are motivated by greed, in some cases, they are motivated by disdain for a certain social order, and in some cases, they commit crimes to prove their mental superiority(Kremling & Sharp Parker, 2017). To illustrate the severity of cybercrime, it is enough to cite a few examples of what crimes cybercriminals commit: sexual violence against minors in cyberspace (Martellozzo, 2017), racism (Cleland, 2017), online bullying of minors (Kowalski et al., 2014), Some organized crime syndicates use cyberspace to carry out their criminal activities(Lavorgna, 2020). The list is incomplete since as a result of technological development, the possible actions to be carried out in cyberspace are inexhaustible. This research paper will show in detail what new ways cybercriminals are finding to carry out their criminal activities in the virtual world, cyberspace. Criminal actions can be directed against individuals or populations, as well as small companies, some large organizations, and even countries.

For the present scientific research, the researcher studied the modern scientific literature, the analysis of which showed what types of cybercrimes take place in reality, for what purposes cybercriminals use cyberspace, and

what problems the law enforcement structures face in the process of battling cybercrime, accordingly what are the megatrends and grand challenges of cybercrime(Koops, 2016). As a result, after studying the mentioned problems, the researcher analyzed the modern legal bases and showed that one of the problems that arise in the process of fighting against cybercrime is the outdated legal bases that cannot effectively respond to the challenges needed to fight against cybercrime(Guinchard, 2020).

There is a fair opinion that when discussing cybercrimes, even today, no attention is paid to how serious a crime cybercrime is. In certain circles, where old legal opinions and dogmatics reign, it is believed that law, throughout its development, is at a height to respond to every new challenge, be it cybercrime or any other crime. It is easy to understand that such an approach makes the fight against cybercrimes much more difficult, because cybercrime is the so-called "crime of the future", which has not yet completed its development, and each researcher, as the author of this scientific paper, must be updated daily and must spread knowledge so that everyone will be ready for the challenges that will take place in the near future (Choraś et al., 2016).

Based on all of the above, in the final part of the scientific research, the author will summarize the examined and analyzed literature, and will highlight the news that exists around cybercrime, what problems investigators face when investigating the "crime of the future". Researcher will present the minimum recommendations that each country should share, so that the fight against cybercrime will be fast and effective. With the appropriate legal framework and preparation from law enforcement structures, any "crime of the future" can be defeated, without problems and difficulties (Chawki et al., 2015b).

The meaning and danger of the cybercrime

As stated in the introduction, cybercrime is the "crime of the future". The mentioned crime received a similar status because the areas of the mentioned illegal action have not yet been defined (Hill & Marion, 2016). For example, a few years ago, no one would have thought that cyberspace would be an important place for terrorists, where they would manage to launder money and sow fear and panic among the population. No one would have thought that there would be such a currency that did not have a physical face. Therefore, cyberspace is a space that is still not fully explored and cybercrime is a crime that is progressing day by day (T. J. Holt & Bossler, 2017).

First of all, it is important to define what cybercrime is. After all, without defining the crime, it will be difficult to fight against it, because it cannot be distinguished from other crimes (Payne, 2020). When

investigating cybercrime, law enforcement structures must take into account several details, that were not taken into mind in the recent past, because the threat of cybercrime was not perceived as real and was seen as an event that would take place in the distant future. Although it must be said that, some researchers talked about the fact, That there are crimes for which computer devices are used, not the methods of the past e.g.: criminals using cyberspace to launder money (Richards, 2006).

As it was said, no one believed the ideas of those researchers. However, it soon turned out that cybercrime cases increased and the law enforcement structures were not ready to fight against it (Bandler & Merzon, 2020). e.g. It took a long time to arrest the famous cybercriminal, Max Butler. During the time Butler was free, he earned millions of dollars through illegal activities in cyberspace (Poulsen, 2011). Had the law enforcement structures been ready, and if they had listened to researchers, who said that computer technologies evolved and could be used for criminal purposes, Butler's criminal act would have been prevented long before he would have managed to cause such significant damage.

Cybercrime, by its very nature, is a type of crime that always takes place in cyberspace, and the perpetrator uses computer devices to carry out his criminal act (Clough, 2015). In the early period, the main goal of cybercriminals was to steal money, money laundering, i.e. to carry out actions related to material wealth. But, along with technological development, law enforcement structures already have to deal with new types of cybercrimes against which there are still no appropriate legal bases to fight against. It is welcome that there are certain conventions and cybercrime is regulated in the national legislation of certain countries, however, as it appeared in the literature studied for the research, the general legal regulation of cybercrime is not enough to effectively combat the said crime. It is necessary to re-examine each crime. Lawyers must understand that espionage and cyber espionage are different crimes and that cyber espionage cannot be effectively combated in the same way that espionage is combated (Dimaggio, 2022). It is also important to remember that cyber espionage is not the only new type of cybercrime, everyone must remember for example Cyberterrorism (Ariu et al., 2016) or Cyberwarfare (Bernik, 2014). For example, to understand how dangerous cyber-espionage is, it is enough to imagine that, from anywhere in the world, a person with a computer device can gain access to the state secrets of any country, and if those secrets are made public, it is easy to imagine what the consequences could be. When, on the contrary, in the case of classic espionage, it is necessary to carry out certain actions, establish contacts, etc. for the spy to obtain the secrets necessary for his purposes.

It is also important to note that some states do not take the dangers coming from cyberspace seriously and believe that they are already safe. For example, the police in many cases use social networks to introduce certain types of information to the public and thus assist citizens, which is important. although the study rightly notes that, in certain cases, police officers may violate certain safety norms, which may raise new problems (Nhan & Noakes, 2020). Also, in the recent past, several cyber-attacks took place, through which the work of specific state structures was disrupted, and this was because in many cases the simplest security norms were neglected, and people were thinking that using some kind of antivirus is enough (Cybersecurity awareness: A Real-World Perspective on Cybercrime & Cyberattacks, n.d.). In the era of technological revolution, one of the ancient sayings that the fittest will survive, is not true anymore, because in the modern world, in modern conditions, those who adapt to the technological revolution will survive(Jenkinson, 2022). Each person, especially those who hold an official position, should remember that it is extremely significant for them to observe the minimum safety standards so that their ill-considered actions do not lead to harmful consequences.

It is significant to understand, what kind of dangers can be faced by a person who spends even a small part of his day in cyberspace. People for whom the norms of morality are alien will use every opportunity to carry out their criminal activity and harm the interests of a particular person. For example, some cybercriminals try to obtain footage of the private life of victims to take revenge or simply to destroy their reputation in cyberspace or reality (K. Holt & Liggett, 2020), or use the same footage by threatening to spread and sexually assault the victim (Powell et al., 2019). It is also noted that cases of sexual harassment occur quite often in cyberspace, both against adults (Chawki et al., 2015d) and minors (Chawki et al., 2015c). A timely investigation is important so that a person feels safe, whose goal is to simply pass the time by surfing the virtual space. It is also very important to find timely psychological or relevant help for the victims of such crimes because becoming a victim of a crime and at the same time having the details of the crime known to the whole society is psychologically difficult for many people to bear. Therefore, the timely help found for them is of special importance in many cases(Vincent, 2017).

Also, the fact is that most humans use the Internet, therefore they have access to cyberspace. With this knowledge, terrorist groups use cyberspace for their purposes (Jerman-Blažič & Klobučar, 2016). The implementation of a terrorist act has not taken place in cyberspace, however, the distribution of video and photo materials depicting terrorist acts carried out by them to cause fear and panic in the population is quite common (Owen et al., 2017a). It is also noted that, for the law enforcement forces, the

fight against the terrorist threat coming from space is connected with difficulties, due to the problems that are on the agenda. Therefore, counter-cyber terrorists need to have methods and arsenal to be able to fight against serious crimes like cyber terrorism (Kijewski et al., 2016).

Of course, the new types of cybercrime listed in this paper is not complete for person to have a complete idea of the dangers of cybercrime, however, even this small list will give a clear idea to the researcher to know what cybercrime is and what serious dangers it carries. Therefore, each person should remember to follow the minimum safety standards while in cyberspace, so they will not become a victim of cybercriminals (Waschke, 2017). In modern times, the protection means on computer systems are not strong enough to ensure the security, anonymity and privacy of ordinary users (Chawki et al., 2015a), especially if it is taken into account that, in many cases, ordinary users, due to stories read on the Internet, are connecting to places such as the so-called Cybercriminal Platform - DarkNet (Liggett et al., 2019). While in cyberspace, each person should remember that they leave some traces that can be used by cybercriminals. Therefore, even for basic protection, people should not go to the darknet, but also they should not access doubtful websites, if their security and privacy are important to them (Augenbaum, 2019). The techniques used by cybercriminals today are so rich that even the slightest trace left while surfing the Internet can cause irreparable harm to a person.

As it was said, it is true that cybercrime is one of the most serious crimes, because in many cases it is difficult to determine what kind of real damage can occur, but a more serious crime is falsely accusing an innocent person. Cybercriminals have tools in their arsenal, using which they can leave a false trail and the investigation will arrest someone who has nothing to do with the crime. Therefore, in each specific case, it is important to study the case in detail, so that the intolerant fight against cybercrime does not become an excuse for violating the rights of innocent people (Maillart, 2021).

Problems in the process of investigating cybercrime

Talking about the importance of cybercrime, it has been repeatedly said that there are a number of problems surrounding the mentioned crime. First of all, the problem to be understood is that for the majority of lawyers, the terminology used to regulate the cyberspace and therefore cybercrime is incomprehensible to them, it is not possible to understand what this or that term means, and because of this, it is difficult for them to fully study the issue. Of course, there is literature with the help of which it is possible to study the issues surrounding cyberspace, however, such literature is written in technical language typical for specialists in the field, and not in popular

language, so that representatives of humanitarian sciences can easily understand the issues (Alexandrou, 2021). It follows logically that if the issue is not fully studied and understood, it will be incredibly difficult to legally regulate it. Regulating this or that action, when the content is not fully and absolutely understandable to the lawyer, is associated with problems.

Of course, for the purposes of scientific research, the current legal frameworks were studied, e.g. the European Union Convention on Cybercrime (de Arimatéia da Cruz, 2020), the legislation of the United States of America on the fight against cybercrime (Bossler, 2020) or the Budapest Convention on the Legal Regulation of Cybercrime (Chang, 2020). Researcher studied cybercrime in the national legislation of certain countries. And there was also a study of European public-private partnerships strategies in the process of fighting against cybercrime (Olesen, 2016).

At first glance, based on the abundance of similar legal acts, the reader may be left with the impression that the fight against cybercrime is effective and there are no problems on the agenda, because there is such a rich legal base. However, it should not be forgotten which legislative framework is effective in combating crime: the legislative framework is effective and strong in crime prevention when it responds to modern challenges, and in the case of cybercrime, responds to the rapid pace of technological progress. Therefore, the existing legal framework is welcomed as a great step towards progress, although modernity shows that the said legal framework is outdated and needs revision to respond to new challenges (Guinchard, 2020). As mentioned in the first paragraph of this chapter, it is rightly noted that, despite the fact that there are many opinions around cybercrime and many studies are conducted, the majority of lawyers do not understand what cybercrime is and what it actually represents: a crime committed by computer technology (McGuire, 2019).

In the process of fighting against crime, a number of new sciences have been formed, with the help of which, the fighters against crime have an arsenal, which can be used to effectively prevent or investigate crimes. One of these sciences is criminology, which terminologically means the science of the crime. With the help of existing theories in criminology, it becomes easier to determine what problems exist in society, what crimes certain elements of society are prone to commit, what crimes are likely to be committed, etc. That is, with the help of the science of criminology, some kind of deterrent combat strategies are determined by the relevant structures. There was an opinion that the use of criminology methods and strategies would be effective against cybercrime, however, as practice has shown, cyberspace is a new, different phenomenon, one can say a new society, which needs different models and strategies to study. The models that exist

in the science of modern criminology have not been found to be effective against cyberspace, cybercrime and cybercriminals. The researcher rightly pointed out that in criminology it is necessary to form a new direction "virtual criminology" (McCarthy & Steinmetz, 2020).

The mentioned opinion was accepted by the legal circles, because it is really necessary to have a similar direction in criminology to fight against cybercrimes. However, it is rightly noted that, as of today, "virtual criminology" methods and strategies are not effective enough to successfully combat cybercrime cases (Owen et al., 2017b). However, as for any science, it is important not to stop working on it and deepen the knowledge so that in the future there will be strategies that will help the law enforcement structures to successfully fight against cybercrimes. Even at first, the science of criminology was not effective, and in certain legal circles it was believed that the science of criminology had no future, because such a science would never become an aid in the process of fighting crime. Modernity shows that the last opinion was not valid, and the science of criminology is one of the greatest aids in the process of fighting crime. It is for this reason that it is important not to stop working on the development of a new direction of criminology called "virtual criminology".

It should be noted here that in the past there were a number of crimes, the investigation of which was associated with certain difficulties, however, along with technological development, new tools, methods and strategies were born. Investigating similar crimes today is no longer associated with any difficulties, because investigators, scientists, lawyers did not give up and developed the aforementioned arsenal. A similar situation exists around the investigation of cybercrimes. Investigating cybercrimes nowadays is very difficult, because in many cases it is necessary to search for traces not in the real world, but in the virtual world. Searching for traces in the latter requires special knowledge, which in many cases is not related to the legal world (Edwards, 2019).

In the presence of outdated legal frameworks around cybercrime, as well as in the absence of methods and strategies to effectively investigate cybercrime, there is also one important detail to be considered, which is called spending of budget funds. A really logical and valid idea is raised in the study that if there are no methods and models in the law enforcement structures, with the help of which the fight against cybercrime will be fast and effective, the funds in the budget are wasted, because the money is spent, but the desired result is not achieved (Armin et al ., 2016). In the presence of effective methods and strategies, as well as a legal framework that responds to modern challenges, less money will be spent in the process of battle against cybercrimes, the remaining amount will be used in other fields, which are no less necessary to develop.

Based on all of the above, it is important for lawyers to study cybercrime, not only from a legal point of view, but also from the point of view of other sciences, in order to fully understand what cybercrime is and who is a cybercriminal (Ghosh & Turrini, 2014, Maimon, 2020). A number of studies have pointed out that the cybercriminal is a new type of criminal who in many cases does not need to take any action other than to use a keyboard. And what kind of damage he can do with one keyboard is easy to guess. Viewing cybercrime from the angle of psychological science, from the angle of computer science or from the angle of philosophical science will be of great help to lawyers to formulate such a legal framework that will respond to the challenges of today and will be directed towards the challenges of the future. And it will provide assistance to the representatives of ordinary law enforcement structures in the process of fighting against cybercrime (Dodge & Burruss, 2019).

In addition to studying cybercrime from a multidisciplinary point of view, it will also provide significant help to lawyers to study and analyze existing theories (Chawki et al., 2015e, Mehan, 2014). Also, it is noteworthy to study the existence of such methods, which are not legally regulated, but, in the case of legal regulation, can provide the greatest assistance to the representatives of the relevant force structure in the process of fighting cybercrime (T. J. Holt, 2019). In many cases, it is possible that one theory, taken separately, may not be the bearer of a significant load, but synthesizing, analyzing and adapting several theories to modern challenges will be of great importance in the process of fighting against such a serious crime as cybercrime.

Conclusions and recomendations

The aim of the research of this scientific article is to present what cybercrime is, what dangers it carries and what new types of cybercrime exist. For the purposes of the study, the author of the scientific article studied the opinions of dozens of scientists on cybercrime, cyberspace and cyber security, and as a result of the analysis, it appeared that there are a number of problems on the agenda that complicate the effective and rapid fight against cybercrime, which consequently leads to severe consequences, on the one hand, cybercriminals feel unpunished, On the other hand, the number of victims of crime is increasing.

One of the biggest problems that emerged in the research is that most of the lawyers do not know the concept and meaning of cybercrime and they are satisfied with the knowledge that is written in the disposition of the law. As it appeared in the research, the mentioned is not enough to make the fight against cybercrime effective. In the research, it appeared that in order to understand the meaning and complexity of cybercrime, it is necessary to

study the crime not only from a legal point of view, but also from the point of view of other sciences, so that lawyers have a complete idea of what cyberspace is, what kind of crime cybercrime is and who is the perpetrator of cybercrime.

Such problems are the reason why the existing legal frameworks cannot respond to the challenges of the modern technological revolution. In the study, it was noted that, in terms of legislative regulation, two main problems appeared:

The first problem is that the existing regulations are outdated and cannot respond effectively to modern challenges.

The second problem is that there are a number of cybercrimes that are not regulated at the legal level at all.

The fact is the following: the types of cybercrime and the arsenal of cybercriminals are becoming richer every day, on the contrary, the arsenal of the relevant structures fighting against them is outdated, which is why an effective and decisive fight against cybercrime cannot be carried out.

By understanding and analyzing the problems presented in the scientific research, the author of the study has recommendations, the understanding and sharing of which will be a step forward in the process of fighting against cybercrime:

1. First of all, which is of particular importance, it is necessary to update the existing legal bases in order to effectively respond to modern challenges. Also, it is important to initiate new legislation to make the fight against new types of cybercrimes more effective.
2. It is necessary to conduct trainings or organize informative meetings, where persons with legal education will get detailed knowledge about computer sciences.
3. It is important to have international partnerships with different countries in order to share experience in the fight against cybercrime.
4. Meetings with security experts are needed so that lawyers will know what kind of protection norms need to be implemented to protect confidential or other information from cybercriminals.
5. It is necessary to develop the direction of virtual criminology.

In summary, it can be said that cybercrime is definitely one of the most dangerous crimes against which humanity is fighting. Due to the fact that cybercrime is the latest form of crime, and also considering that new types of cybercrime appear on the agenda, it is important to solve the problems presented in the research in a timely manner to make the fight against cybercrime more effective and intolerant. Implementation of the

recommendations presented in the scientific article will be an important step towards the elimination of problems, which will lead to the reduction and timely prevention of cybercrime cases. In such a situation, the main goal, which should be important for every country, will be achieved: protection of citizens' security privacy and rights.

References:

1. Alexandrou, A. (2021). Cybercrime and information technology: Theory and practice: The computer network infrastructure and computer security, cybersecurity laws, internet of things (IoT), and mobile devices. CRC Press.
2. Ariu, D., Didaci, L., Fumera, G., Giacinto, G., Roli, F., Frumento, E., & Freschi, F. (2016). A (cyber)ROAD to the future: A methodology for building cybersecurity research roadmaps. In Advanced Sciences and Technologies for Security Applications (pp. 53–77). Springer International Publishing.
3. Armin, J., Thompson, B., & Kijewski, P. (2016). Cybercrime economic costs: No measure no solution. In Advanced Sciences and Technologies for Security Applications (pp. 135–155). Springer International Publishing.
4. Augenbaum, S. (2019). The secret to cybersecurity the secret to cybersecurity: A simple plan to protect your family and business from cybercrime. Forefront Books.
5. Bandler, J., & Merzon, A. (2020). Cybercrime investigations: A comprehensive resource for everyone. CRC Press.
6. Bernik, I. (2014). Cybercrime and Cyber Warfare (1st ed.). ISTE Ltd and John Wiley & Sons.
7. Bossler, A. M. (2020). Cybercrime legislation in the United States. In The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 257–280). Springer International Publishing.
8. Chang, L. Y. C. (2020). Legislative frameworks against cybercrime: The Budapest convention and Asia. In The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 327–343). Springer International Publishing.
9. Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015a). Anonymity, privacy and security issues in cyberworld. In Studies in Computational Intelligence (pp. 97–111). Springer International Publishing.
10. Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015b). Cybercrime: Introduction, Motivation and Methods. In Studies in Computational Intelligence (pp. 3–23). Springer International Publishing.

11. Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015c). Online obscenity and child sexual abuse. In Studies in Computational Intelligence (pp. 81–94). Springer International Publishing.
12. Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015d). Sexual Harassment in Cyberworld. In Studies in Computational Intelligence (pp. 65–78). Springer International Publishing.
13. Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015e). Strategies and statutes for prevention of cybercrime. In Studies in Computational Intelligence (pp. 113–127). Springer International Publishing.
14. Choi, K.-S., Lee, C. S., & Louderback, E. R. (2020). Historical evolutions of cybercrime: From computer crime to cybercrime. In The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 27–43). Springer International Publishing.
15. Choraś, M., Kozik, R., Churchill, A., & Yautsiukhin, A. (2016). Are we doing all the right things to counter cybercrime? In Advanced Sciences and Technologies for Security Applications (pp. 279–294). Springer International Publishing.
16. Cleland, J. (2017). Online racial hate speech. In Cybercrime and its Victims (1st Edition, pp. 131–147). Routledge.
17. Clough, J. (2015). Principles of Cybercrime (2nd ed.). Cambridge University Press.
18. Cybersecurity awarness: A Real-World Perspective on Cybercrime & Cyberattacks. (n.d.). Pothi.com. Retrieved August 20, 2022, from https://store.pothi.com/book/ebook-prakash-prasad-cybersecurity-awarness-real-world-perspective-cybercrime-cyberattacks /de Arimatéia da Cruz, J. (2020). The legislative framework of the European union (EU) convention on cybercrime. In The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 223–237). Springer International Publishing.
19. Dimaggio, J. (2022). The art of cyberwarfare the art of cyberwarfare: An investigator's guide to espionage, ransomware, and organized cybercrime. No Starch Press.
20. Dodge, C., & Burruss, G. (2019). Policing cybercrime. In The Human Factor of Cybercrime (1st Edition, pp. 339–358). Routledge.
21. Ec-Council. (2016). Computer forensics: Investigating network intrusions and cybercrime (chfi), 2nd edition (2nd ed.). Cengage Learning.
22. Edwards, G. (2019). Cybercrime Investigators Handbook. Standards Information Network.
23. Ghosh, S., & Turrini, E. (Eds.). (2014). Cybercrimes: A Multidisciplinary Analysis (2011th ed.). Springer.

24. Guinchard, A. (2020). The criminalisation of tools under the computer misuse act 1990. The need to rethink cybercrime offences to effectively protect legitimate activities and deter cybercriminals. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3865146
25. Hill, J. B., & Marion, N. E. (2016). Introduction to cybercrime: Computer crimes, laws, and policing in the 21st century: Computer crimes, laws, and policing in the 21st century. Praeger.
26. Holt, K., & Liggett, R. (2020). Revenge Pornography. In The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 1–19). Springer International Publishing.
27. Holt, T. J. (2019). Police and Extralegal Structures to Combat Cybercrime. In The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 1–18). Springer International Publishing.
28. Holt, T. J., & Bossler, A. M. (2017). Cybercrime in Progress: Theory and prevention of technology-enabled offenses. Routledge.
29. Hutchings, A., Pastrana, S., & Clayton, R. (2019). Displacing big data. In The Human Factor of Cybercrime (1st Edition, pp. 408–424). Routledge.
30. Jenkinson, A. (2022). Ransomware and Cybercrime. Taylor & Francis.
31. Jerman-Blažič, B., & Klobučar, T. (2016). Towards the development of a research agenda for cybercrime and cyberterrorism – identifying the technical challenges and missing solutions. In Advanced Sciences and Technologies for Security Applications (pp. 157–174). Springer International Publishing.
32. Kijewski, P., Jaroszewski, P., Urbanowicz, J. A., & Armin, J. (2016). The never-ending game of cyberattack attribution. In Advanced Sciences and Technologies for Security Applications (pp. 175–192). Springer International Publishing.
33. Koops, B.-J. (2016). Megatrends and grand challenges of cybercrime and cyberterrorism policy and research. In Advanced Sciences and Technologies for Security Applications (pp. 3–15). Springer International Publishing.
34. Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: a critical review and meta-analysis of cyberbullying research among youth. Psychological Bulletin, 140(4), 1073–1137. https://doi.org/10.1037/a0035618
35. Kremling, J., & Sharp Parker, A. M. (2017). Cyberspace, Cybersecurity, and Cybercrime. SAGE Publications.
36. Lavorgna, A. (2020). Organized Crime and Cybercrime. In The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 117–134). Springer International Publishing.

37. Liggett, R., Lee, J. R., Roddy, A. L., & Wallin, M. A. (2019). The dark web as a platform for crime: An exploration of illicit drug, firearm, CSAM, and cybercrime markets. In The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 1–27). Springer International Publishing.
38. Maillart, J.-B. (2021). The need to think beyond objective territoriality to better protect the rights of the suspect of a cybercrime. In Rethinking Cybercrime (pp. 105–120). Springer International Publishing.
39. Maimon, D. (2020). Deterrence in cyberspace: An interdisciplinary review of the empirical literature. In The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 1–19). Springer International Publishing.
40. Marion, N. E., & Twede, J. (2020). Cybercrime: An Encyclopedia of Digital Crime. ABC-CLIO.
41. Martellozzo, E. (2017). Online sexual grooming. In Cybercrime and its Victims (1st Edition, pp. 108–128). Routledge.
42. McCarthy, A. L., & Steinmetz, K. F. (2020). Critical Criminology and Cybercrime. In The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 601–621). Springer International Publishing.
43. McGuire, M. (2019). It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime. In The Human Factor of Cybercrime (1st Edition, pp. 3–28). Routledge.
44. Mehan, J. E. (2014). Cyberwar, cyberterror, cybercrime and cyberactivism: An in-depth guide to the role of standards in the cybersecurity environment (2nd ed.). IT Governance Publishing.
45. Nhan, J., & Noakes, N. (2020). Police legitimacy in the age of the internet. In The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 403–424). Springer International Publishing.
46. Olesen, N. (2016). European public-private partnerships on cybersecurity - an instrument to support the fight against cybercrime and cyberterrorism. In Advanced Sciences and Technologies for Security Applications (pp. 259–278). Springer International Publishing.
47. Owen, T., Noble, W., & Speed, F. C. (2017a). Something you wish you had never seen – videos of death & murder on Facebook, you tube and other media platforms. In New Perspectives on Cybercrime (pp. 241–252). Springer International Publishing.
48. Owen, T., Noble, W., & Speed, F. C. (2017b). The problem of 'virtual criminology.' In New Perspectives on Cybercrime (pp. 177–196). Springer International Publishing.

49. Payne, B. K. (2020). Defining Cybercrime. In The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 3–25). Springer International Publishing.
50. Poulsen, K. (2011). Kingpin. Crown Publishing Group.
51. Powell, A., Flynn, A., & Henry, N. (2019). Sexual violence in digital society. In The Human Factor of Cybercrime (1st Edition, pp. 134–155). Routledge.
52. Richards, J. R. (2006). Transnational criminal organizations, cybercrime, and money laundering: A handbook for law enforcement officers, auditors, and financial investigators (2nd ed.). CRC Press.
53. Vincent, N. A. (2017). Victims of cybercrime: definitions and challenges. In Cybercrime and its victims (pp. 27–42). Routledge, Taylor and Francis Group.
54. Waschke, M. (2017). Personal cybersecurity: How to avoid and recover from cybercrime (1st ed.). APRESS.